James Bugel
Assistant Vice President
Public Safety and
Homeland Security

AT&T Services Inc.
1120 20th Street, NW
Suite 1000
Washington, DC 20036

T: 202.457-2052
F: 202-457-2008

December 18, 2009

EX PARTE NOTICE

Ms. Marlene H. Dortch
Secretary,
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

In re: 700 MHz Interoperable Broadband Public Safety Network
PS Docket No. 06-229; WT Docket No. 06-150

Dear Ms. Dortch:

On December 17th, 2009, Stacey Black, Assistant Vice President of AT&T Services, Inc. ("AT&T"), Dr. David Shively, Lead Member of Technical Staff of AT&T Services and the undersigned met with Behzad Ghaffari, Kurian Jacob, Jerry Stanshine, Jeff Cohen of the Public Safety Homeland and Security Bureau and Tom Peters of the Office of Strategic Planning to discuss additional efforts that can be taken to encourage the creation of a contiguous 20 MHz block of broadband spectrum for use by public safety.

In May 2009, eight major public safety agencies announced a "consensus position" to "petition Congress to reallocate the 700 MHz D-Block creating a single 20 MHz block of broadband spectrum for use by public safety." In addition, the National Emergency Number Association (NENA) has recently indicated support for this consensus position after exploring a full array of alternative solutions. AT&T has already noted the importance of having the full 20 MHz in previous filings as a critical requirement, unique to public safety, given their ever-expanding need for data applications. Indeed, AT&T believes that securing this spectrum for public safety in perpetuity is the highest calling and best use of this 20 MHz block and that this opportunity represents a once in a lifetime chance to get it right for the public safety community. As AT&T has noted in previous filings, we have experienced a 5000% increase in data traffic in the last 3 years and it shows no sign of slowing. In fact, all evidence points to increased data usage and an accelerated growth rate. AT&T described research and provided statistics on wireless data usage for its government data customers. As AT&T testified during the recent House Subcommittee hearing, we found that data usage of the government segment, which includes public safety, has grown from 11 MB per month per user in 2005 to nearly 200 MB per month, per user. (See addendum).

As an illustrative example of this increase in monthly data usage, the City of Mountain View, California, has shared information that it has collected over the last few years regarding the accelerated growth in data usage among its public safety vehicles. Mountain View is a moderately sized city and its experience is representative of the scale of data traffic growth that can be expected throughout the United States. The City reports that total consumption of

wireless data on the AT&T Mobility network has increased over 500% over the past three years, primarily driven by the introduction of new systems and applications for public safety use. The following facts provide a glimpse into the City's experience:

	October 2006	October 2009
Number of Devices	34	39
Total Usage	382 Megabytes	2,365 Megabytes
Average Use Per Device	11.2 Megabytes	60.1 Megabytes

- The Fire Department's incident command vehicle, which also has access to the public Internet consistently uses 200-300 Megabytes per month.

- Applications that are already deployed:

  - Automated Field Reporting (AFR): Officers compose and upload their crime, traffic collision, and miscellaneous service reports via the wireless network, while supervisors download, review and approve these reports without having to drive to the police station.

  - Online resources: The City of Mountain View provides access to hosted peace officer resource information via a 3rd party provider. Access to California Penal and Vehicle Code resources, as well as the California Peace Officer Legal Sourcebook are now provided via the wireless network, rather than loading a separate application on each mobile computer. The City also allows public safety users to access Internal City systems such as e-mail and the City's Intranet, via the wireless network.

  - Regional and state systems: Authorized users now access the County of Santa Clara booking ("mugshot") photo system, as well as the State of California's "CalPhoto" system via the wireless network, providing them with access to DMV driver license photograph database, as well as booking photos from many other California counties.

  - License Plate Recognition (LPR) systems: Like many law enforcement agencies, we have deployed this technology, and use the AT&T wireless network to transfer large amounts of data to/from our LPR-equipped vehicles. Average monthly data consumption for these vehicles is ~ 700 Megabytes per month.

  - Regional Fire/EMS mutual aid/healthcare system: The Mountain View Fire Department incident commander accesses a regional web-based portal to review and update Fire/EMS mutual aid resources.

The City of Mountain View has told us that its consumption of wireless data will continue to grow as it introduces more applications, such as automated vehicle location and location based services, in-car video systems, in-field biometric identification devices, and electronic citation

systems, and grants access to those applications to its public safety users. The addition of these applications will most likely drive their wireless data usage closer to 300 MB per month, per user, as the Florida Department of Highway Safety & Motor Vehicles ("Florida State Patrol") is currently experiencing. The Florida State Patrol's use of digital photography, facial recognition and streaming audio and video applications for both law enforcement and training activities has driven its average wireless data usage per user to around 340 MB per month. AT&T believes that these types of applications and corresponding data use will likely be repeated by other state and local public safety agencies throughout the county, demonstrates the need for the federal government to take a long-term view of public safety's spectrum needs and to plan for these substantial increases in wireless data usage. Public safety must be insulated from problems resulting from unrestrained growth on commercial spectrum by deploying its own network utilizing dedicated nationwide spectrum. This in turn will drive both public and private sector job creation and expansion as these networks are built out in local communities all over America. It also provides federal users with the opportunity to utilize these networks in a cost effective manner, thereby significantly reducing the burden to the taxpayer.

Analogies can be drawn from many others areas of public infrastructure. For example, the U.S. Interstate Highway system was constructed after considering and accounting for future automobile traffic capacity needs. Nevertheless, automobile traffic has outgrown the highway capacity in many areas and costly expansions and renovations are being made. Further, deploying government services, such as light rail, or utilities, such as water and electricity, requires an initial infrastructure investment based upon the anticipated future demands for the service. Failing to take into account reasonably anticipated future demand during the initial investment phase would result in significant additional costs to upgrade and increase capacity in the system, such as costs to lay additional tracks or to run additional electrical lines. Spectrum for public safety is no different than these examples. If we fail to scale properly, congestion, blocking, and inadequate capacity in a national emergency would result, which would only serve to multiply the effects of a disaster due to lack of adequate communication and information. The Commission must seize this opportunity to give public safety the spectrum it needs to protect our citizens in times of emergency. If we fail to do so, it may be impossible to allocate another contiguous block of spectrum with the technical synergies and cost effectiveness that is present with the 700 MHz D-Block to effectively deploy the network needed by public safety. In addition, without adequate spectrum, the additional capacity that will be needed will have to result in continued cell-splitting which will increase the cost and complexities for the public safety network.

AT&T characterizes public safety as a unique data user in that during an incident or emergency, network demand is typically concentrated in a small geographic area. While commercial carriers can deploy and provision additional capacity at pre-planned events, public safety will not have the luxury of planning the next disaster or incident that will likely involve multiple jurisdictions in a defined geographic area. Consequently, the additional 10 MHz will provide critical capacity when needed. The attached slide showing multiple users per sector concentration and available bandwidth in 5 MHz, 10 MHz, and 20 MHZ implementations indicates how easily a site could become congested during a moderate emergency with multiple

public safety users downloading data and clearly demonstrates the need for the full 20 MHz block of spectrum.

It has been suggested that the reallocating the existing 12 MHz of narrowband public safety spectrum for broadband use is a viable option. However, this narrowband reallocation is not viable and should not be considered for the following reasons:

- Millions of dollars have already been spent in implementing traditional land mobile public safety voice systems in the narrowband spectrum and many more are already planned. To stop that progress would be disastrous to the public safety community and the communities they serve.

- In the near term, wireless broadband cannot replace the current Land Mobile Radio (LMR) mission critical public safety voice systems currently in use...

- Current and planned broadband standards and technologies depend on a network approach while public safety must also have a non-network capability to communicate in emergencies when a network cannot be reached or is out of service.

- Before LMR systems could be supplanted, broadband services would first need to be deployed to the level that provides the same extensive coverage that mission critical voice systems provide, including in-building coverage.

The steps taken by public safety entities, public safety organizations, and the Public Safety Spectrum Trust, including the recent waiver requests seeking authorization to use the public safety broadband spectrum, bring us closer than ever to the Commission's goal of an interoperable broadband network with high bandwidth technologies for use by first responders and other public safety professionals. But, this goal cannot become a reality without the combined efforts of Congress, the Commission, public safety, wireless carriers, and device manufacturers. The following steps must be taken:

- The Commission should support public safety's request that Congress reallocate the 700 MHz D-Block spectrum to public safety. The 700 MHz D-Block spectrum is public safety's last opportunity for building a cost effective, interoperable broadband network for the 21st Century.

- Congress should allow public safety to use new or existing grant programs to fund the purchase of dedicated RAN equipment and managed broadband services. This is especially important for rural public safety agencies.

- The Commission should grant waiver requests by public safety entities to deploy networks on the 700 MHz public safety broadband spectrum and establish minimum standards for those broadband networks to ensure interoperability, including an endorsement of LTE as the standard technology, as recommended by the public safety community

- The Commission, following Congressional reallocation, should grant 20 MHz broadband licenses to local or regional public safety applicants wishing to begin build out of their networks.

- Wireless carriers can aid and support the expansion of public safety CPE by encouraging the development of devices utilizing Band 14 chipsets that are supported by the LTE standard.

- Wireless carriers and public safety can collaborate to best leverage the benefits of commercial core networks.

Pursuant to Section 1.1206 of the Commission's rules, an electronic copy of this letter is being filed for inclusion in the above-referenced docket.

Respectfully Submitted,

Jim Bugel
Assistant Vice President
Public Safety and Homeland Security
AT&T Services, Inc.
1120 20th Street, N.W.
Suite 1000
Washington, D.C. 20036

Attachment

cc: Jennifer Manner
Behzad Ghaffari
Kurian Jacob
Jerry Stanshine
Jeff Cohen
Tom Peters